(19) (11) Publication number: 08160857 A

Generated Document.

PATENT ABSTRACTS OF JAPAN

(21) Application number: 06323921

(22) Application date: 30.11.94

(51) Intl. Cl.: G09C 1/00 H04L 9/00 H04L 9/10 H04L 9/12

(30) Priority:

(43) Date of application publication: 21.06.96

(84) Designated contracting states:

(71) Applicant: HITACHI LTD

(72) Inventor: NISHIOKA GENJI

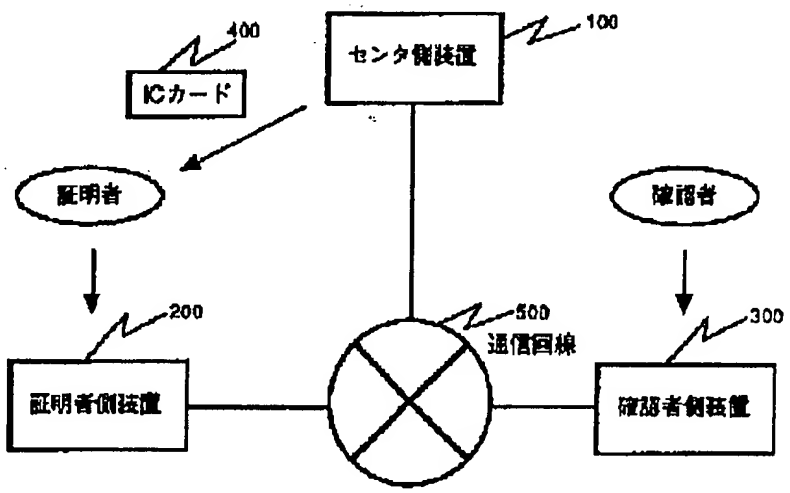
(74) Representative:

(54) AUTHENTICATION METHOD AND SYSTEM BASED ON ELLIPTIC CURVE

(57) Abstract:

PURPOSE: To provide a zero knowledge authentication system which is used to authenticate identity, for example, and has higher safety as compared with the zero knowledge authentication system based on the discrete logarithmic problem on a finite body without reducing the authentication processing effi ciency.

CONSTITUTION: The authentication protocol for a discrete logarithmic problem on an elliptic curve, which is more difficult than the discrete logarithmic problem on a finite body, is constructed as a cryptographical assumption. An elliptic curve E and an addition on the curve E are defined beforehand. The curve E and points P and Q on the curve E are disclosed at a center 100 and an integer x is distributed to a verifier at the center 100. In the center 100, x satisfies Q=xP (where xP means multiplication calculation that P is added x times to the point P on the curve E) for the points P and Q on the curve E and the verifier authenticates that a confirmor has the without leaking the knowledge relative to x.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平8－160857

(43)公開日　平成８年(1996)６月21日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ	1/00		7259－5Ｊ		
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
				Ｈ０４Ｌ　9/00	Ｚ

審査請求　未請求　請求項の数８　ＦＤ　（全 15 頁）

(21)出願番号　特願平6－323921

(22)出願日　平成６年(1994)11月30日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

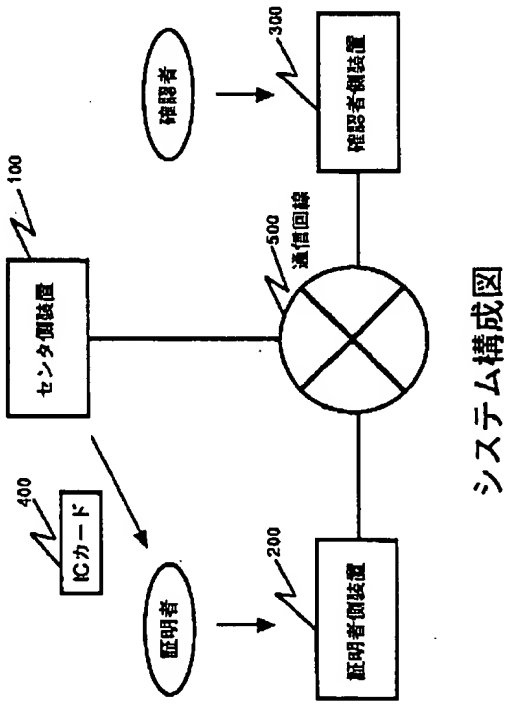
(74)代理人　弁理士　矢島　保夫

(54)【発明の名称】　楕円曲線に基づく認証方法及び認証システム

(57)【要約】　（修正有）

【目的】身元を証明するような認証システムにおいて、有限体上の離散対数問題に基づく零知識認証方式に比べ、認証処理効率を下げることなく、安全性のより高い零知識認証方式を提案する。

【構成】有限体上の離散対数問題よりも難しい問題である楕円曲線上の離散対数問題を暗号学的仮定として認証プロトコルを構築する。予め楕円曲線Ｅ及び該楕円曲線Ｅ上における加法を定義しておき、センタにおいて該楕円曲線Ｅ及び該楕円曲線Ｅ上の点Ｐ、Ｑを公開し、センタにおいて上記楕円曲線Ｅ上の点Ｐ、Ｑに関し、Ｑ＝ｘＰ（ただしｘＰは、楕円曲線Ｅ上の点Ｐに対して、Ｐをｘ回加える倍計算を意味する）を満足する整数ｘを証明者に配布し、証明者が確認者に対してｘを所持することをｘに関する知識を漏らすことなく証明することにより、認証を行なう。



システム構成図

1

【特許請求の範囲】

【請求項1】証明者が確認者に対して自分の身元を証明する目的で信頼できるセンタを訪れ、センタが作成した証明者用の秘密の情報を利用して、証明者が確認者に身元を証明する認証方法であって、

予め、楕円曲線E、及び該楕円曲線E上における加法を定義しておくステップと、

センタにおいて、該楕円曲線E、及び該楕円曲線E上の点P，Qを公開するステップと、

センタにおいて、上記楕円曲線E上の点P，Qに関し、

$Q=xP$　（ただしxPは、楕円曲線E上の点Pに対して、Pをx回加える倍計算を意味する）

を満足する整数xを証明者に配布するステップと、

証明者が、確認者に対して、xを所持することをxに関する知識を漏らすことなく証明することにより、認証を行なうステップとを備えたことを特徴とする認証方法。

【請求項2】証明者が確認者に対して自分の身元を証明する目的で信頼できるセンタを訪れ、センタが作成した証明者用の秘密の情報を利用して、証明者が確認者に身元を証明する認証方法であって、

センタにおける準備処理として、

秘密情報s（ただし、sは$0<s<q$なる整数）を生成して保持するステップと、

素数p，q、楕円曲線E、及び該楕円曲線E上の点G，V（ただし、$V=sG$で、sGは楕円曲線E上において定義された加法により、Gをs回加える倍計算を意味する）を生成して公開するステップとを備え、

証明者のセンタへの登録処理として、

証明者からセンタに、該証明者のＩＤ情報ID_Aを送るステップと、

センタにおいて、乱数t_A（ただし、t_Aは$0<t_A<q$なる整数）、センタの秘密情報s、並びに、センタの公開情報である素数p，q、楕円曲線E、及び該楕円曲線E上の点G，Vを用いて、

$z_AG=(ID_A+x_A)V+X_A$

を満足する楕円曲線E上の点$X_A=t_AG=(x_A, y_A)$と$0<z_A<q$なる整数z_Aを作成し、X_Aとz_Aを認証用の情報として証明者に配付するステップとを備え、

証明者と確認者の間の認証処理として、

証明者から確認者に、ＩＤ情報ID_Aと$X_A=(x_A, y_A)$とを送るステップと、

（i）証明者は、$0<r_i<q$なる整数r_iをランダムに選び、楕円曲線E上の点U_iを

$U_i=r_iG$

にて計算し、U_iを確認者に送る；

（ii）確認者は、$e_i \in R$（ただし、Rは素体Z_qの適当な部分集合）をランダムに選び、e_iを証明者に送る；

（iii）証明者は、

$w_i=r_i+e_iz_A \pmod q$

を計算して、w_iを確認者に送る；

2

（iv）確認者は、

$U_i=w_iG-e_i((ID_A+x_A)V+X_A)$

が成立することを確かめる；上記（i）～（iv）をi＝1からt（tはセキュリティパラメータ）まで繰り返すことにより、証明者の認証を行なうステップとを備えたことを特徴とする認証方法。

【請求項3】証明者が確認者に対して自分の身元を証明する目的で信頼できるセンタを訪れ、センタが作成した証明者用の秘密の情報を利用して、証明者が確認者に身元を証明する認証方法であって、

センタにおける準備処理として、

秘密情報s（ただし、sは$0<s<q$なる整数）を生成して保持するステップと、

素数p，q、楕円曲線E、及び該楕円曲線E上の点G，V（ただし、$V=sG$で、sGは楕円曲線E上において定義された加法により、Gをs回加える倍計算を意味する）を生成して公開するステップとを備え、

証明者のセンタへの登録処理として、

証明者からセンタに、該証明者のＩＤ情報ID_Aを送るステップと、

センタにおいて、乱数t_A（ただし、t_Aは$0<t_A<q$なる整数）、センタの秘密情報s、並びに、センタの公開情報である素数p，q、楕円曲線E、及び該楕円曲線E上の点G，Vを用いて、

$z_AG=(ID_A+x_A)V+X_A$

を満足する楕円曲線E上の点$X_A=t_AG=(x_A, y_A)$と$0<z_A<q$なる整数z_Aを作成し、X_Aとz_Aを認証用の情報として証明者に配付するステップとを備え、

証明者と確認者の間の認証処理として、

証明者から確認者に、ＩＤ情報ID_Aと$X_A=(x_A, y_A)$とを送るステップと、

（i）証明者は、$0<r_i<q$なる整数r_iをランダムに選び、整数u_iを

$u_i=(r_iG)_x$

にて計算し、u_iを確認者に送る（ただし、括弧の右下にxを付した表記は括弧内の点のx座標を表わし、射影平面で定義された楕円曲線E上の点$P=(x:y:z)$に対して、$z\neq 0$のとき、点Pのx座標$(P)_x$は$(P)_x=x/z$であるものとする）；

（ii）確認者は、$e_i \in R$（ただし、Rは素体Z_qの適当な部分集合）をランダムに選び、e_iを証明者に送る；

（iii）証明者は、

$w_i=r_i+e_iz_A \pmod q$

を計算して、w_iを確認者に送る；

（iv）確認者は、

$u_i=(w_iG-e_i((ID_A+x_A)V+X_A))_x$

が成立することを確かめる；上記（i）～（iv）をi＝1からt（tはセキュリティパラメータ）まで繰り返すことにより、証明者の認証を行なうステップとを備えたことを特徴とする認証方法。

3

【請求項4】証明者が確認者に対して自分の身元を証明する目的で信頼できるセンタを訪れ、センタが作成した証明者用の秘密の情報を利用して、証明者が確認者に身元を証明する認証方法であって、

センタにおける準備処理として、

秘密情報s（ただし、sは0＜s＜qなる整数）を生成して保持するステップと、

素数p，q、正定数r（r≦q）、楕円曲線E、及び該楕円曲線E上の点G，V（ただし、V＝sGで、sGは楕円曲線E上において定義された加法により、Gをs回加える倍計算を意味する）を生成して公開するステップとを備え、

証明者のセンタへの登録処理として、

証明者からセンタに、該証明者のID情報ID_Aを送るステップと、

センタにおいて、乱数t_A（ただし、t_Aは$0<t_A<q$なる整数）、センタの秘密情報s、並びに、センタの公開情報である素数p，q、正定数r、楕円曲線E、及び該楕円曲線E上の点G，Vを用いて、

$y_A G=(ID_A+x_A)V+X_A$

を満足する楕円曲線E上の点$X_A=t_A G=(a_x, a_y)$、$x_A=a_x \pmod r$、及び、$0<y_A<q$なる整数y_Aを作成し、X_Aとy_Aを認証用の情報として証明者に配付するステップとを備え、

証明者と確認者の間の認証処理として、

証明者から確認者に、ID情報ID_Aと$X_A=(x_A, y_A)$とを送るステップと、

（i）証明者は、$0<r_i<q$なる整数r_iをランダムに選び、整数u_iを

$u_i=(r_i G)_x \pmod r$

にて計算し、u_iを確認者に送る（ただし、括弧の右下にxを付した表記は括弧内の点のx座標を表わし、射影平面で定義された楕円曲線E上の点P＝（x：y：z）に対して、$z\neq 0$のとき、点Pのx座標$(P)_x$は$(P)_x=x/z$であるものとする）；

（ii）確認者は、$e_i \in R$（ただし、Rは素体Z_qの適当な部分集合）をランダムに選び、e_iを証明者に送る；

（iii）証明者は、

$w_i=r_i+e_i y_A \pmod q$

を計算して、w_iを確認者に送る；

（iv）確認者は、

$u_i=(w_i G-e_i((ID_A+x_A)V+X_A))_x \pmod r$

が成立することを確かめる；上記（i）～（iv）をi＝1からt（tはセキュリティパラメータ）まで繰り返すことにより、証明者の認証を行なうステップとを備えたことを特徴とする認証方法。

【請求項5】証明者が確認者に対して自分の身元を証明する目的で信頼できるセンタを訪れ、センタが作成した証明者用の秘密の情報を利用して、証明者が確認者に身元を証明する認証方法であって、

4

センタにおける準備処理として、

秘密情報s（ただし、sは0＜s＜qなる整数）を生成して保持するステップと、

素数p，q、楕円曲線E、及び該楕円曲線E上の点G，V（ただし、V＝sGで、sGは楕円曲線E上において定義された加法により、Gをs回加える倍計算を意味する）を生成して公開するステップとを備え、

証明者のセンタへの登録処理として、

証明者からセンタに、該証明者のID情報ID_Aを送るステップと、

センタにおいて、乱数t_A（ただし、t_Aは$0<t_A<q$なる整数）、センタの秘密情報s、並びに、センタの公開情報である素数p，q、楕円曲線E、及び該楕円曲線E上の点G，Vを用いて、

$z_A X_A=ID_A G+x_A V$

を満足する楕円曲線E上の点$X_A=t_A G=(x_A, y_A)$と$0<z_A<q$なる整数z_Aを作成し、X_Aとz_Aを認証用の情報として証明者に配付するステップとを備え、

証明者と確認者の間の認証処理として、

証明者から確認者に、ID情報ID_Aと$X_A=(x_A, y_A)$とを送るステップと、

（i）証明者は、$0<r_i<q$なる整数r_iをランダムに選び、楕円曲線E上の点U_iを

$U_i=r_i X_A$

にて計算し、U_iを確認者に送る；

（ii）確認者は、$e_i \in R$（ただし、Rは素体Z_qの適当な部分集合）をランダムに選び、e_iを証明者に送る；

（iii）証明者は、

$w_i=r_i+e_i z_A \pmod q$

を計算して、w_iを確認者に送る；

（iv）確認者は、

$U_i=w_i X_A-e_i(ID_A G+x_A V)$

が成立することを確かめる；上記（i）～（iv）をi＝1からt（tはセキュリティパラメータ）まで繰り返すことにより、証明者の認証を行なうステップとを備えたことを特徴とする認証方法。

【請求項6】証明者が確認者に対して自分の身元を証明する目的で信頼できるセンタを訪れ、センタが作成した証明者用の秘密の情報を利用して、証明者が確認者に身元を証明する認証方法であって、

センタにおける準備処理として、

秘密情報s（ただし、sは0＜s＜qなる整数）を生成して保持するステップと、

素数p，q、楕円曲線E、及び該楕円曲線E上の点G，V（ただし、V＝sGで、sGは楕円曲線E上において定義された加法により、Gをs回加える倍計算を意味する）を生成して公開するステップとを備え、

証明者のセンタへの登録処理として、

証明者からセンタに、該証明者のID情報ID_Aを送るステップと、

5

センタにおいて、乱数t_A（ただし、t_Aは$0<t_A<q$なる整数）、センタの秘密情報s、並びに、センタの公開情報である素数p，q、楕円曲線E、及び該楕円曲線E上の点G，Vを用いて、

$z_A G=(ID_A+x_A)V+X_A$

を満足する楕円曲線E上の点$X_A=t_A G=(x_A, y_A)$と$0<z_A<q$なる整数z_Aを作成し、X_Aとz_Aを認証用の情報として証明者に配付するステップとを備え、

証明者と確認者の間の認証処理として、

証明者から確認者に、ＩＤ情報ID_Aと$X_A=(x_A, y_A)$とを送るステップと、

（ｉ）証明者は、$0<r_i<q$なる整数r_iをランダムに選び、整数u_iを

$u_i=(r_i X_A)_x$

にて計算し、u_iを確認者に送る（ただし、括弧の右下にxを付した表記は括弧内の点のｘ座標を表わし、射影平面で定義された楕円曲線E上の点$P=(x:y:z)$に対して、$z\neq 0$のとき、点Pのｘ座標$(P)_x$は$(P)_x=x/z$であるものとする）；

（ii）確認者は、$e_i \in R$（ただし、Rは素体Z_qの適当な部分集合）をランダムに選び、e_iを証明者に送る；

（iii）証明者は、

$w_i=r_i+e_i z_A \pmod q$

を計算して、w_iを確認者に送る；

（iv）確認者は、

$u_i=(w_i X_A-e_i(ID_A G+x_A V))_x$

が成立することを確かめる；上記（ｉ）～（iv）をｉ＝１からｔ（ｔはセキュリティパラメータ）まで繰り返すことにより、証明者の認証を行なうステップとを備えたことを特徴とする認証方法。

【請求項７】証明者が確認者に対して自分の身元を証明する目的で信頼できるセンタを訪れ、センタが作成した証明者用の秘密の情報を利用して、証明者が確認者に身元を証明する認証方法であって、

センタにおける準備処理として、

秘密情報ｓ（ただし、ｓは$0<s<q$なる整数）を生成して保持するステップと、

素数p，q、正定数ｒ（$r \leqq q$）、楕円曲線E、及び該楕円曲線E上の点G，V（ただし、$V=sG$で、ｓGは楕円曲線E上において定義された加法により、Gをｓ回加える倍計算を意味する）を生成して公開するステップとを備え、

証明者のセンタへの登録処理として、

証明者からセンタに、該証明者のＩＤ情報ID_Aを送るステップと、

センタにおいて、乱数t_A（ただし、t_Aは$0<t_A<q$なる整数）、センタの秘密情報ｓ、並びに、センタの公開情報である素数p，q、正定数ｒ、楕円曲線E、及び該楕円曲線E上の点G，Vを用いて、

$z_A X_A=ID_A G+x_A V$

6

を満足する楕円曲線E上の点$X_A=t_A G=(a_x, a_y)$、$x_A=a_x \pmod r$、及び、$0<y_A<q$なる整数y_Aを作成し、X_Aとy_Aを認証用の情報として証明者に配付するステップとを備え、

証明者と確認者の間の認証処理として、

証明者から確認者に、ＩＤ情報ID_Aと$X_A=(x_A, y_A)$とを送るステップと、

（ｉ）証明者は、$0<r_i<q$なる整数r_iをランダムに選び、整数u_iを

$u_i=(r_i X_A)_x \pmod r$

にて計算し、u_iを確認者に送る（ただし、括弧の右下にxを付した表記は括弧内の点のｘ座標を表わし、射影平面で定義された楕円曲線E上の点$P=(x:y:z)$に対して、$z\neq 0$のとき、点Pのｘ座標$(P)_x$は$(P)_x=x/z$であるものとする）；

（ii）確認者は、$e_i \in R$（ただし、Rは素体Z_qの適当な部分集合）をランダムに選び、e_iを証明者に送る；

（iii）証明者は、

$w_i=r_i+e_i y_A \pmod q$

を計算して、w_iを確認者に送る；

（iv）確認者は、

$u_i=(w_i X_A-e_i(ID_A G+x_A V))_x \pmod r$

が成立することを確かめる；上記（ｉ）～（iv）をｉ＝１からｔ（ｔはセキュリティパラメータ）まで繰り返すことにより、証明者の認証を行なうステップとを備えたことを特徴とする認証方法。

【請求項８】証明者が確認者に対して自分の身元を証明する目的で信頼できるセンタを訪れ、センタが作成した証明者用の秘密の情報を利用して、証明者が確認者に身元を証明する認証システムにおいて、

予めセンタ側装置において、楕円曲線E、及び該楕円曲線E上における加法を定義する手段と、

センタ側装置において定義した楕円曲線E、及び該楕円曲線E上の点P，Qを公開情報として証明者側装置及び確認者側装置に送る手段と、

センタ側装置において、上記楕円曲線E上の点P，Qに関し、

$Q=xP$　（ただしｘPは、楕円曲線E上の点Pに対して、Pをｘ回加える倍計算を意味する）

を満足する整数ｘを証明者に配布する手段と、

証明者側装置と確認者側装置との間で、証明者が、確認者に対して、ｘを所持することをｘに関する知識を漏らすことなく証明することにより、認証を行なう手段とを備えたことを特徴とする認証システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、楕円曲線に基づく認証方式及び装置に関し、特に情報セキュリティの分野において、証明者が確認者に対して自分の身元の正当性を証明する認証技術に関する発明である。

【0002】

【従来の技術】近年、暗号の分野では、公開鍵暗号の安全性をより高めることを主な目的として、有限体上の問題（例えば、離散対数問題）を楕円曲線上の問題に置き換えて暗号アルゴリズムを構築する試みが起ってきた。

【0003】そこで、まず楕円曲線の基本的事項について説明し、さらに楕円曲線上の離散対数問題の困難性に安全性の根拠を置くDiffie-Hellmannタイプの鍵共有方式について説明する。

【0004】Kを体とする。このとき、$P=(a_0, a_1, \cdots, a_n)$，$Q=(b_0, b_1, \cdots, b_n) \in K^{n+1}-\{(0, 0, \cdots, 0)\}$ に対して、関係～を次の様に定義する。

$P \sim Q \Leftrightarrow \exists \lambda \neq 0 \in K$ s.t $a_i=\lambda b_i$ for $i=0, \cdots, n$

なお、記号⇔は、定義を意味するものとする。

【0005】このとき、関係～は同値関係になり、商空間$(K^{n+1}-\{(0, 0, \cdots, 0)\})/\sim$をn次元射影空間（n＝2のとき、射影平面）と呼び、$P^n(K)$、または、単にP^nで表わす。また、P^nにおいて、$P=(a_0, a_1, \cdots, a_n)$を代表元とする同値類を$(a_0 : a_1 : \cdots : a_n)$と書き、$P=(a_0 : a_1 : \cdots : a_n)$で表わす。さらに、$P^n$の部分空間 $\{(a_0 : a_1 : \cdots : a_n) \in P^n \mid X_{n+1}=0\}$ を無限遠超平面（n＝2のときは、無限遠直線）と呼ぶ。

【0006】体Kの標数が3より大きいとき、K上の楕円曲線$E_K(a, b)$を次の様に定義する。

【0007】$E_K(a, b)=\{(x : y : z) \in P^2 \mid y^2 z=x^3+axz^2+bz^3, 4a^3+27b^2 \neq 0, a, b \in K\}$

また、$E=E_K(a, b)$と無限遠直線との交点$(0 : 1 : 0)$を無限遠点と呼び、Oによって表わす。

【0008】このとき、定義から、楕円曲線$E_K(a, b)$は、

$E_K(a, b)=\{(x, y) \in K^2 \mid y^2=x^3+ax+b, 4a^3+27b^2 \neq 0, a, b \in K\} \cup O$

と表わすこともできる（以降、簡単のため、この表記をとる）。

【0009】K上の楕円曲線Eにおいて、次の（1）から（4）のように加法＋を定義する。このとき、（E, +）はアーベル群をなす。

【0010】（1）P＝O，Q∈Eのとき、－P＝O，P＋Q＝Qとする。すなわち、無限遠点Oを単位元とする。

【0011】（2）P＝（x，y）∈Eのとき、－P＝（x，－y）とする。

【0012】（3）Q＝－Pのとき、P＋Q＝Oとする。

【0013】（4）$P=(x_1, y_1)$，$Q=(x_2, y_2) \in E$に対して、$P+Q=(x_3, y_3)$を、

$x_3=\lambda^2-x_1-x_2$

$y_3=-y_1+\lambda(x_1-x_3)$

により、定義する。ただし、

$\lambda=(y_2-y_1)/(x_2-x_1)$ if $x_1 \neq x_2$

$(3x_1^2+a)/2y_1$ if $P=Q$

とする。

【0014】素体Z_p（素数pを法とする剰余体）上の楕円曲線$E=E_p(a, b)$とB∈Eにおいて、（Bをベースとする）E上の離散対数問題とは、「P∈Eが与えられたとき、P＝xBを満たす整数xを求めよ。」なる問題を意味する。ただし、xBとは、E上において定義された加法の下で、Bをx回加える倍計算を意味する。また、位数がqのP∈Eに対して、すなわち、xP＝Oとなる最小の正数xがqとなるP∈Eに対して、Nを整数nを代表元とするZ_qの元とするとき、NP＝nPと定義できることに注意する。

【0015】一般に、楕円曲線上の離散対数問題のほうが、有限体上の離散対数問題よりも難しい問題であると予想されている。

【0016】体上の離散対数問題に基づくDiffie-Hellmann鍵配送方式は、公開鍵暗号の概念を実現する具体的な方法として良く知られている。次に、文献「N.Koblitz: Elliptic Curve Cryptosystems; Mathematics of Computation, Vol.48 (1987)」に記載の楕円曲線版Diffie-Hellmann鍵配送方式について説明する。

【0017】センタの公開情報を用いて、AとBが鍵共有する場合を考える。

【0018】1．センタの準備処理

センタは、素数pとZ_p上の楕円曲線を表わす係数部のパラメータ（a，b）、及び、位数がqとなる楕円曲線上のベース点Pを定めて、A及びBに公開する。

【0019】2．鍵共有処理

1）Aは$s_A \in Z_q$をランダムに選び、

$C_A=s_A P$

を計算し、点C_AをBに送る。Bは$s_B \in Z_q$をランダムに選び、

$C_B=s_B P$

を計算し、点C_BをAに送る。

【0020】2）AはC_Bとs_Aから鍵K_{AB}を、

$K_{AB}=s_A C_B$

と計算する。BはC_Aとs_Bから鍵K_{BA}を、

$K_{BA}=s_B C_A$

と計算する。

【0021】このとき、$K_{AB}=K_{BA}$が成立し、AとBの間で鍵共有が行なわれたことになる。

【0022】

【発明が解決しようとする課題】高度情報化社会においては、通信ネットワーク上で、電子投票を行なったり重要な契約などを行なう等のほか、様々なサービスが行なわれることが予想される。この際、ネットワークの利用者が自分の身元を安全に相手に証明する認証技術が必要

不可欠になる。

【0023】また、今後は、大きな加入者数を持つネットワークが増えるものと予想され、センタの集中管理が難しくなると考えられる。そこで、大規模分散環境下での使用を前提とした高安全・高効率の認証技術が要求される。

【0024】零知識証明を用いた認証方式は、認証プロトコルから秘密情報を漏らさないことが保証されている安全性の高い認証方式であるが、さらに、証明者のＩＤ情報とセンタの公開情報のみで認証処理を行なうことができるため、公開鍵ファイルの必要がなく、また、センタの負荷が少なくなる点において、大規模分散環境下に適した認証方式の１つである。

【0025】しかし、従来の零知識証明が暗号学的仮定としている有限体上の離散対数問題や平方剰余問題については、コンピュータの計算処理能力の向上やアルゴリズムの研究に伴い、問題のサイズを大きくする必要が生じている。

【0026】本発明の目的は、センタが作成した認証用の秘密情報を利用して、証明者が確認者に対して自分の身元を証明する認証システムにおいて、従来知られている零知識認証方式に比べ、より難しい問題を暗号学的仮定とする効率の良い零知識認証方式、及び、装置を提供することにある。

【0027】

【課題を解決するための手段】本発明は、零知識証明を用いた認証方式のさらなる安全性の向上を目的として、楕円曲線上の離散対数問題に基づく零知識認証方式を提案するものである。すなわち、本発明では、予め楕円曲線Ｅ及び該楕円曲線Ｅ上における加法を定義しておき、センタにおいて該楕円曲線Ｅ及び該楕円曲線Ｅ上の点Ｐ，Ｑを公開し、センタにおいて上記楕円曲線Ｅ上の点Ｐ，Ｑに関し、Ｑ＝ｘＰ（ただしｘＰは、楕円曲線Ｅ上の点Ｐに対して、Ｐをｘ回加える倍計算を意味する）を満足する整数ｘを証明者に配布し、証明者が確認者に対してｘを所持することをｘに関する知識を漏らすことなく証明することにより、認証を行なう。

【0028】具体的実現方法の１つとしては、センタにおける準備処理として、秘密情報ｓ（ただし、ｓは０＜ｓ＜ｑなる整数）を生成して保持するステップと、素数ｐ，ｑ、楕円曲線Ｅ、及び該楕円曲線Ｅ上の点Ｇ，Ｖ（ただし、Ｖ＝ｓＧで、ｓＧは楕円曲線Ｅ上において定義された加法により、Ｇをｓ回加える倍計算を意味する）を生成して公開するステップとを備え、証明者のセンタへの登録処理として、証明者からセンタに、該証明者のＩＤ情報ID_Aを送るステップと、センタにおいて、乱数t_A（ただし、t_Aは$0<t_A<q$なる整数）、センタの秘密情報ｓ、並びに、センタの公開情報である素数ｐ，ｑ、楕円曲線Ｅ、及び該楕円曲線Ｅ上の点Ｇ，Ｖを用いて、

$z_A G=(ID_A+x_A)V+X_A$

を満足する楕円曲線Ｅ上の点$X_A=t_A G=(x_A, y_A)$と$0<z_A<q$なる整数z_Aを作成し、X_Aとz_Aを認証用の情報として証明者に配付するステップとを備え、証明者と確認者の間の認証処理として、証明者から確認者に、ＩＤ情報ID_Aと$X_A=(x_A, y_A)$とを送るステップと、

（ｉ）証明者は、$0<r_i<q$なる整数r_iをランダムに選び、楕円曲線Ｅ上の点U_iを

$U_i=r_i G$

にて計算し、U_iを確認者に送る；

（ii）確認者は、$e_i \in R$（ただし、Ｒは素体Z_qの適当な部分集合）をランダムに選び、e_iを証明者に送る；

（iii）証明者は、

$w_i=r_i+e_i z_A \pmod q$

を計算して、w_iを確認者に送る；

（iv）確認者は、

$U_i=w_i G-e_i((ID_A+x_A)V+X_A)$

が成立することを確かめる；上記（ｉ）～（iv）をｉ＝１からｔ（ｔはセキュリティパラメータ）まで繰り返すことにより、証明者の認証を行なうステップとを備えるようにする。

【0029】上記（ｉ）では楕円曲線Ｅ上の点U_iのｘ座標及びｙ座標を証明者から確認者に送り、（iv）で$U_i=w_i G-e_i((ID_A+x_A)V+X_A)$を確かめたが、点$U_i$のｘ座標のみを用いるようにしてもよい。また、所定の正定数ｒを用いて点U_iのｘ座標の（mod ｒ）により確認するようにしてもよい。これらについては、実施例により具体的に説明する。

【0030】

【作用】本発明における認証方式では、楕円曲線上の離散対数問題に基づいて零知識認証スキームを構築している。楕円曲線上の離散対数問題は、有限体Z_p上の離散対数問題よりも難しいと予想されているため、従来方式である体上の離散対数問題に基づく零知識認証方式に比べ、認証スキーム自体の安全性が向上する。さらに、証明者と確認者間の認証プロトコルにおいては、楕円曲線上の点のｘ座標のみの通信内容で認証プロトコルを構築することもできるので、従来方式と同程度の通信量・通信回数で認証処理が実現できる。また、本発明における認証方式では、確認者が証明者を試すために送る乱数の範囲を大きく取れるため、少ない通信回数で不正者の証明者へのなりすまし確率を低く設定することができる。

【0031】

【実施例】以下、図面を用いて、本発明の実施例について詳しく説明する。

【0032】図１は、本発明の一実施例に係る認証システムのシステム構成を示す図である。このシステムは、センタ側装置100と証明者側装置200と確認者側装置300とＩＣカード400とから構成されている。センタ側装置1

00と証明者側装置200と確認者側装置300は、通信回線500を介して接続されている。

【0033】証明者は、確認者に自分の身元を証明することを目的として、認証用の秘密情報を搭載したセンタ発行のICカード400を所持し、このICカード400を利用して証明者側装置200と確認者側装置300との間で通信回線500を介して認証処理を行なう。

【0034】図2は、センタ側装置100の内部構成を示す。センタ側装置100は、入力装置101、演算装置102、メモリ103、乱数生成装置104、素数生成装置105、通信装置106、及び、出力装置107を備えている。

【0035】図3は、証明者側装置200の内部構成を示す。証明者側装置200は、入力装置201、ICカード読み書き装置202、通信装置203、及び、出力装置204を備えている。

【0036】図4は、確認者側装置300の内部構成を示す。確認者側装置300は、入力装置301、演算装置302、メモリ303、乱数生成装置304、通信装置305、及び、出力装置306を備えている。

【0037】図5は、ICカード400の内部構成を示す。ICカード400は、入力装置401、演算装置402、メモリ403、乱数生成装置404、及び、出力装置405を備えている。以下、実施例1～6により具体的な認証の手順について説明する。なお、これらの実施例1～6は、何れも上記図1～図5の構成のシステム上で実現されるものとする。

【0038】（実施例1）証明者は、確認者に対して自分の身元を証明したい。この目的の下で、証明者は信頼できるセンタを訪ねる。

【0039】1．センタの準備処理

センタは、センタ側装置100内の入力装置101と演算装置102とメモリ103と乱数生成装置104と素数生成装置105を用いて、秘密情報と公開情報を次の要領で作成し、通信装置106及び出力装置107を用いて公開情報のみを通信回線500を介して公開する。また、秘密情報はメモリ103に格納する。

【0040】秘密情報：

・$s \in Z$ s.t $0 < s < q$

【0041】公開情報：

・p：512ビット程度の素数

・q：160ビット程度の素数

・$(a, b) \in Z_p^2$ s.t $4a^3 + 27b^2 \neq 0$

・$G \in E$ s.t $ord(G) = q$

・$V = sG \in E$

【0042】ここで、Z_pは素数pを法とする剰余体を表わす。さらに、$(a, b) \in Z_p^2$により、楕円曲線$E = E_p(a, b) = \{(x, y) \in Z_p^2 \mid y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0, a, b \in Z_p\} \cup O$を表わす。また、$P \in E$に対して、$ord(P) = n$とは、Pの位数がnであることを意味する。すなわち、$xP = O$となる最小の正整数xがnである。xPとは、点Pをx回加える倍計算を意味する（計算方法については、「従来の技術」を参照）。特に断わらないかぎり、以降についても同様の表現をとる。

【0043】2．証明者の登録処理

証明者は、確認者に対して自分の身元を証明することを目的にセンタを訪ねる。証明者は、自分のID情報ID_Aをセンタに登録する。センタは、センタ側装置100内の乱数生成装置104を用いて、$0 < t_A < q$なる整数t_Aをランダムに選び、演算装置102及びメモリ103を用いて、楕円曲線E上の点X_Aと整数z_Aを

$X_A = t_A G = (x_A, y_A)$

$z_A = s(ID_A + x_A) + t_A \pmod q$

にて計算する。そして、楕円曲線E上の点X_Aとz_Aと証明者のID情報ID_AをICカード400内のメモリ403に格納して、ICカード400を証明者に配布する。

【0044】3．認証プロトコル

証明者は、証明者側装置200を用いて、確認者側装置300の確認者に対して、通信回線500を介して次のプロトコルを実行することにより、

$z_A G = (ID_A + x_A)V + X_A$

を満足する整数z_Aを所持することを証明する。

【0045】1）証明者は、ICカード400を証明者側装置200内のICカード読み書き装置202に差し込む。ICカード400は、メモリ403に格納されている証明者のID情報ID_Aと$X_A = (x_A, y_A)$を、出力装置405を用いて証明者側装置200に出力する。証明者側装置200は、通信装置203及び出力装置204を用いて通信回線500を介して、ID情報ID_Aと$X_A = (x_A, y_A)$を確認者側装置300に送る。

【0046】次に、2)から5)のステップをi＝1からkまで繰り返し、全てのiについてステップ5)の等式が成立すれば、確認者は証明者を受理する（kはセキュリティパラメータ）。

【0047】2）証明者は、ICカード400内の乱数生成装置404を用いて、$0 < r_i < q$なる整数r_iをランダムに選び、楕円曲線E上の点U_iを

$U_i = r_i G$

にて演算装置402及びメモリ403を用いて計算した後、証明者側装置200に出力し、証明者側装置200内の出力装置203と通信装置204を用いて、通信回線500を介して、U_iを確認者側装置300に送る。

【0048】3）確認者側装置300は、U_iを受信後、U_iをメモリ303に格納し、乱数生成装置304を用いて、乱数$e_i \in R$を選び、通信装置305及び出力装置306を用いて、通信回線500を介して、e_iを証明者側装置200に送る（ただし、RはZ_qの適当な部分集合）。

【0049】4）証明者側装置200は、e_iを受信後、e_iをICカード400内のメモリ403に出力し、ICカード400は演算装置402及びメモリ403を用いて、

$w_i = r_i + e_i z_A \pmod q$

を計算した後、証明者側装置200に出力し、証明者側装置200内の通信装置203及び出力装置204を用いて、通信回線500を介して、w_iを確認者側装置300に送る。

【0050】5）確認者側装置300は、演算装置302及びメモリ303を用いて、

$U_i = w_i G - e_i((ID_A + x_A)V + X_A)$

が成立することを確かめる。

【0051】（実施例2）図6は、実施例2の認証方式の処理手順の概要を示す図である。証明者は、確認者に対して自分の身元を証明したい。この目的の下で、証明者は信頼できるセンタを訪ねる。

【0052】1．センタの準備処理

実施例1と同じ。

【0053】2．証明者の登録処理

実施例1と同じ。

【0054】3．認証プロトコル

証明者は、証明者側装置200を用いて、確認者側装置300の確認者に対して、通信回線500を介して次のプロトコルを実行することにより、

$z_A G = (ID_A + x_A)V + X_A$

を満足する整数z_Aを所持することを証明する。

【0055】1）証明者は、ＩＣカード400を証明者側装置200内のＩＣカード読み書き装置202に差し込む。ＩＣカード400は、メモリ403に格納されている証明者のＩＤ情報ID_Aと$X_A = (x_A, y_A)$を、出力装置405を用いて証明者側装置200に出力する。証明者側装置200は、通信装置203及び出力装置204を用いて通信回線500を介して、ＩＤ情報ID_Aと$X_A = (x_A, y_A)$を確認者側装置300に送る。

【0056】次に、2)から5)のステップを$i = 1$からkまで繰り返し、全てのiについてステップ5)の等式が成立すれば、確認者は証明者を受理する（kはセキュリティパラメータ）。

【0057】2）証明者は、ＩＣカード400内の乱数生成装置404を用いて、$0 < r_i < q$なる整数r_iをランダムに選び、整数u_iを

$u_i = (r_i G)_x$

にて演算装置402及びメモリ403を用いて計算した後、証明者側装置200に出力し、証明者側装置200内の通信装置203と出力装置204を用いて、通信回線500を介して、u_iを確認者側装置300に送る。

【0058】3）確認者側装置300は、u_iを受信後、u_iをメモリ303に格納し、乱数生成装置304を用いて、乱数$e_i \in R$を選び、出力装置305及び通信装置306を用いて、通信回線500を介して、e_iを証明者側装置200に送る（ただし、RはZ_qの適当な部分集合）。

【0059】4）証明者側装置200は、e_iを受信後、e_iをＩＣカード400内のメモリ403に出力し、ＩＣカード400は演算装置402及びメモリ403を用いて、

$w_i = r_i + e_i z_A \pmod q$

を計算した後、証明者側装置200に出力し、証明者側装置200内の通信装置203及び出力装置204を用いて、通信回線500を介して、w_iを確認者側装置300に送る。

【0060】5）確認者側装置300は、演算装置302及びメモリ303を用いて、

$u_i = (w_i G - e_i((ID_A + x_A)V + X_A))_x$

が成立することを確かめる。

【0061】但し、射影平面で定義された楕円曲線上の点$P = (x : y : z)$に対して、$z \neq 0$のとき、$P_x = x/z$とし、Ｐのｘ座標と呼ぶ。以降についても、同様とする。

【0062】上記実施例1では、証明者から確認者に楕円曲線Ｅ上の点U_iのｘ座標及びｙ座標を送り、確認者側でそのｘ座標及びｙ座標について所定の式が成立することを確かめた。これに対し、本実施例2では、証明者から確認者にｘ座標（実施例のu_i）のみを送り、確認者側でそのｘ座標について所定の式が成立することを確かめるようになっている。したがって、実施例1よりも通信路を流れる情報量が少なくなり効率が上がる。

【0063】（実施例3）証明者は、確認者に対して自分の身元を証明したい。この目的の下で、証明者は信頼できるセンタを訪ねる。

【0064】1．センタの準備処理

センタは、センタ側装置内100内の入力装置101と演算装置102とメモリ103と乱数生成装置104と素数生成装置105を用いて、秘密情報と公開情報を次の要領で作成し、通信装置106及び出力装置107を用いて公開情報のみを通信回線500を介して公開する。また、秘密情報はメモリ103に格納する。

【0065】秘密情報：

・$s \in Z$　s.t　$0 < s < q$

【0066】公開情報：

・ｐ：512ビット程度の素数

・ｑ：160ビット程度の素数

・ｒ：$r \leqq q$なる正定数、

・$(a, b) \in Z_p^2$　s.t　$4a^3 + 27b^2 \neq 0$

・$G \in E$　s.t　$ord(G) = q$

・$V = sG \in E$

【0067】2．証明者の登録処理

証明者は、確認者に対して自分の身元を証明することを目的にセンタを訪ねる。証明者は、自分のＩＤ情報ID_Aをセンタに登録する。センタは、センタ側装置100内の乱数生成装置104を用いて、$0 < t_A < q$なる整数t_Aをランダムに選び、演算装置102及びメモリ103を用いて、楕円曲線Ｅ上の点X_Aと整数x_A，y_Aを

$X_A = t_A G = (a_x, a_y)$

$x_A = a_x \pmod r$

$y_A = s(ID_A + x_A) + t_A \pmod q$

にて計算する。そして、X_Aとy_Aと証明者のＩＤ情報ID

$_A$をＩＣカード400内のメモリ403に格納して、ＩＣカード400を証明者に配布する。

【００６８】３．認証プロトコル

証明者は、証明者側装置200を用いて、確認者側装置300の確認者に対して、通信回線500を介して、次のプロトコルを実行することにより、

$y_A G=(ID_A+x_A)V+X_A$

を満足するy_Aを所持することを証明する。

【００６９】１）証明者は、ＩＣカード400を証明者側装置200内のＩＣカード読み書き装置202に差し込む。ＩＣカード400は、メモリ403に格納されている証明者のＩＤ情報ID_Aと$X_A=(a_x, a_y)$を、出力装置405を用いて証明者側装置200に出力する。証明者側装置200は、通信装置203及び出力装置204を用いて、通信回線500を介して、ＩＤ情報ID_Aと$X_A=(a_x, a_y)$を確認者側装置300に送る。

【００７０】次に、2)から5)のステップを$i=1$からｋまで繰り返し、全てのｉについてステップ5)の等式が成立すれば、確認者は証明者を受理する（ｋはセキュリティパラメータ）。

【００７１】２）証明者は、ＩＣカード400内の乱数生成装置404を用いて、$0<r_i<q$なる整数r_iをランダムに選び、整数u_iを

$u_i=(r_i G)_x \pmod r$

にて演算装置402及びメモリ403を用いて計算した後、証明者側装置200に出力し、証明者側装置200内の通信装置203と出力装置204を用いて、通信回線500を介して、u_iを確認者側装置300に送る。

【００７２】３）確認者側装置300は、u_iを受信後、u_iをメモリ303に格納し、乱数生成装置304を用いて、乱数$e_i \in R$を選び、出力装置305及び通信装置306を用いて、通信回線500を介して、e_iを証明者側装置200に送る（ただし、ＲはZ_qの適当な部分集合）。

【００７３】４）証明者側装置200は、e_iを受信後、e_iをＩＣカード400内のメモリ403に出力し、ＩＣカード400は演算装置402及びメモリ403を用いて、

$w_i=r_i+e_i y_A \pmod q$

を計算した後、証明者側装置200に出力し、証明者側装置200内の通信装置203及び出力装置204を用いて、通信回線500を介して、w_iを確認者側装置300に送る。

【００７４】５）確認者側装置300は、演算装置302及びメモリ303を用いて、

$u_i=(w_i G-e_i((ID_A+x_A)V+X_A))_x \pmod r$

が成立することを確かめる。

【００７５】但し、楕円曲線Ｅ上の点Ｐ（≠Ｏ）に対して、$P_x \in Z_q$によりＰのｘ座標を表わす（実施例２参照）。

【００７６】上記実施例２では、証明者から確認者に楕円曲線Ｅ上の点U_iのｘ座標（512ビットのデータ）を送り、確認者側で所定の式が成立することを確かめた。これに対し、本実施例２では、証明者から確認者にｘ座標の(mod r)を取ったデータを送るようにしている。(mod r)を取ることによりデータ値が小さくなるので、通信路を流れる情報量が少なくなり効率が上がる。

【００７７】（実施例４）証明者は、確認者に対して自分の身元を証明したい。この目的の下で、証明者は信頼できるセンタを訪ねる。

【００７８】１．センタの準備処理

センタは、センタ側装置内100内の入力装置101と演算装置102とメモリ103と乱数生成装置104と素数生成装置105を用いて、秘密情報と公開情報を次の要領で作成し、通信装置106および出力装置107を用いて公開情報のみを通信回線500を介して公開する。また、秘密情報はメモリ103に格納する。

【００７９】秘密情報：

・$s \in Z \quad s.t \quad 0<s<q$

【００８０】公開情報：

・ｐ：512ビット程度の素数

・ｑ：160ビット程度の素数

・$(a, b) \in Z_p^2 \quad s.t \quad 4a^3+27b^2 \neq 0$

・$G \in E \quad s.t \quad ord(G)=q$

・$V=sG \in E$

【００８１】２．証明者の登録処理

証明者は、確認者に対して自分の身元を証明することを目的にセンタを訪ねる。証明者は、自分のＩＤ情報ID_Aをセンタに登録する。センタは、センタ側装置100内の乱数生成装置104を用いて、$0<t_A<q$なる整数t_Aをランダムに選び、演算装置102及びメモリ103を用いて、楕円曲線Ｅ上の点X_Aと整数z_Aを

$X_A=t_A G=(x_A, y_A)$

$z_A=(ID_A+s x_A)/t_A \pmod q$

にて計算する。そして、X_Aとz_Aと証明者のＩＤ情報ID_AをＩＣカード400内のメモリ403に格納して、ＩＣカード400を証明者に配布する。

【００８２】３．認証プロトコル

証明者は、証明者側装置200を用いて、確認者側装置300の確認者に対して、通信回線500を介して、次のプロトコルを実行することにより、

$z_A X_A=ID_A G+x_A V$

を満足するz_Aを所持することを証明する。

【００８３】１）証明者は、ＩＣカード400を証明者側装置200内のＩＣカード読み書き装置202に差し込む。ＩＣカード400は、メモリ403に格納されている証明者のＩＤ情報ID_Aと$X_A=(x_A, y_A)$を、出力装置405を用いて証明者側装置200に出力する。証明者側装置200は、出力装置203及び通信装置204を用いて、通信回線500を介して、ＩＤ情報ID_Aと$X_A=(x_A, y_A)$を確認者側装置300に送る。

【００８４】次に、2)から5)のステップを$i=1$からｋまで繰り返し、全てのｉについてステップ5)の等式

が成立すれば、確認者は証明者を受理する（kはセキュリティパラメータ）。

【0085】2）証明者は、ICカード400内の乱数生成装置404を用いて、$0<r_i<q$なる整数r_iをランダムに選び、楕円曲線E上の点U_iを

$U_i=r_iX_A$

にて演算装置402及びメモリ403を用いて計算した後、証明者側装置200に出力し、証明者側装置200内の出力装置203と通信装置204を用いて、通信回線500を介して、U_iを確認者側装置300に送る。

【0086】3）確認者側装置300は、U_iを受信後、U_iをメモリ303に格納し、乱数生成装置304を用いて、乱数$e_i\in R$を選び、出力装置305及び通信装置306を用いて、通信回線500を介して、e_iを証明者側装置200に送る（ただし、RはZqの適当な部分集合）。

【0087】4）証明者側装置200は、e_iを受信後、e_iをICカード400内のメモリ403に出力し、ICカード400は演算装置402及びメモリ403を用いて、

$w_i=r_i+e_iz_A \pmod q$

を計算した後、証明者側装置200に出力し、証明者側装置200内の出力装置203及び通信装置204を用いて、通信回線500を介して、w_iを確認者側装置300に送る。5）確認者側装置300は、演算装置302及びメモリ303を用いて、

$U_i=w_iX_A-e_i(ID_AG+x_AV)$

が成立することを確かめる。

【0088】（実施例5）図7は、実施例5の認証方式の処理手順の概要を示す図である。証明者は、確認者に対して自分の身元を証明したい。この目的の下で、証明者は信頼できるセンタを訪ねる。

【0089】1．センタの準備処理

実施例4と同じ。

【0090】2．証明者の登録処理

実施例4と同じ。

【0091】3．認証プロトコル

証明者は、証明者側装置200を用いて、確認者側装置300の確認者に対して、通信回線500を介して、次のプロトコルを実行することにより、

$z_AX_A=ID_AG+x_AV$

を満足するz_Aを所持することを証明する。

【0092】1）証明者は、ICカード400を証明者側装置200内のICカード読み書き装置202に差し込む。ICカード400は、メモリ403に格納されている証明者のID情報ID_Aと$X_A=(x_A, y_A)$を、出力装置405を用いて証明者側装置200に出力する。証明者側装置200は、出力装置203及び通信装置204を用いて、通信回線500を介して、ID情報ID_Aと$X_A=(x_A, y_A)$を確認者側装置300に送る。

【0093】次に、2)から5)のステップをi＝1からkまで繰り返し、全てのiについてステップ5)の等式が成立すれば、確認者は証明者を受理する（kはセキュリティパラメータ）。

【0094】2）証明者は、ICカード400内の乱数生成装置404を用いて、$0<r_i<q$なる整数r_iをランダムに選び、整数u_iを

$u_i=(r_iX_A)_x$

にて演算装置402及びメモリ403を用いて計算した後、証明者側装置200に出力し、証明者側装置200内の出力装置203と通信装置204を用いて、通信回線500を介して、u_iを確認者側装置300に送る。

【0095】3）確認者側装置300は、u_iを受信後、u_iをメモリ303に格納し、乱数生成装置304を用いて、乱数$e_i\in R$を選び、出力装置305及び通信装置306を用いて、通信回線500を介して、e_iを証明者側装置200に送る（ただし、RはZqの適当な部分集合）。

【0096】4）証明者側装置200は、e_iを受信後、e_iをICカード400内のメモリ403に出力し、ICカード400は演算装置402及びメモリ403を用いて、

$w_i=r_i+e_iz_A \pmod q$

を計算した後、証明者側装置200に出力し、証明者側装置200内の出力装置203及び通信装置204を用いて、通信回線500を介して、w_iを確認者側装置300に送る。

【0097】5）確認者側装置300は、演算装置302及びメモリ303を用いて、

$u_i=(w_iX_A-e_i(ID_AG+x_AV))_x$

が成立することを確かめる。

【0098】但し、楕円曲線E上の点P（≠O）に対して、$P_x\in Z_q$によりPのx座標を表わす（実施例2参照）。

【0099】（実施例6）証明者は、確認者に対して自分の身元を証明したい。この目的の下で、証明者は信頼できるセンタを訪ねる。

【0100】1．センタの準備処理

センタは、センタ側装置内100内の入力装置101と演算装置102とメモリ103と乱数生成装置104と素数生成装置105を用いて、秘密情報と公開情報を次の要領で作成し、通信装置106および出力装置107を用いて公開情報のみを通信回線500を介して公開する。また、秘密情報はメモリ103に格納する。

【0101】秘密情報：

・$s\in Z$ s.t $0<s<q$

【0102】公開情報：

・p：512ビット程度の素数

・q：160ビット程度の素数

・r：$r\leqq q$なる正定数、

・$(a, b)\in Z_p^2$ s.t $4a^3+27b^2\neq 0$

・$G\in E$ s.t $ord(G)=q$

・$V=sG\in E$

【0103】2．証明者の登録処理

証明者は、確認者に対して自分の身元を証明することを

目的にセンタを訪ねる。証明者は、自分のＩＤ情報ID_Aをセンタに登録する。センタは、センタ側装置100内の乱数生成装置104を用いて、$0<t_A<q$なる整数t_Aをランダムに選び、演算装置102及びメモリ103を用いて、楕円曲線Ｅ上の点X_Aと整数x_A，y_Aを

$X_A=t_AG=(a_x, a_y)$

$x_A=a_x \pmod r$

$y_A=(ID_A+s\,x_A)/t_A \pmod q$

にて計算し、X_Aとy_Aと証明者のＩＤ情報ID_AをＩＣカード400内のメモリ403に格納して、ＩＣカード400を証明者に配布する。

【０１０４】３．認証プロトコル

証明者は、証明者側装置200を用いて、確認者側装置300の確認者に対して、通信回線500を介して、次のプロトコルを実行することにより、

$y_AX_A=ID_AG+x_AV$

を満足するy_Aを所持することを証明する。

【０１０５】１）証明者は、ＩＣカード400を証明者側装置200内のＩＣカード読み書き装置202に差し込む。ＩＣカード400は、メモリ403に格納されている証明者のＩＤ情報ID_Aと$X_A=(a_x, a_y)$を、出力装置405を用いて証明者側装置200に出力する。証明者側装置200は、出力装置203及び通信装置204を用いて、通信回線500を介して、確認者側装置300に送る。

【０１０６】次に、２)から５)のステップを$i=1$からｋまで繰り返し、全てのｉについてステップ５)の等式が成立すれば、確認者は証明者を受理する（ｋはセキュリティパラメータ）。

【０１０７】２）証明者は、ＩＣカード400内の乱数生成装置404を用いて、$0<r_i<q$なる整数r_iをランダムに選び、整数u_iを

$u_i=(r_iX_A)_x \pmod r$

にて演算装置402及びメモリ403を用いて計算した後、証明者側装置200に出力し、証明者側装置200内の出力装置203と通信装置204を用いて、通信回線500を介して、u_iを確認者側装置300に送る。

【０１０８】３）確認者側装置300は、u_iを受信後、u_iをメモリ303に格納し、乱数生成装置304を用いて、乱数$e_i \in R$を選び、出力装置305及び通信装置306を用いて、通信回線500を介して、e_iを証明者側装置200に送る（ただし、ＲはZ_qの適当な部分集合）。

【０１０９】４）証明者側装置200は、e_iを受信後、e_iをＩＣカード400内のメモリ403に出力し、ＩＣカード400は演算装置402及びメモリ403を用いて、

$w_i=r_i+e_iy_A \pmod q$

を計算した後、証明者側装置200に出力し、証明者側装置200内の出力装置203及び通信装置204を用いて、通信回線500を介して、w_iを確認者側装置300に送る。

【０１１０】５）確認者側装置300は、演算装置302及びメモリ303を用いて、

$u_i=(w_iX_A-e_i(ID_AG+x_AV))_x \pmod r$

が成立することを確かめる。

【０１１１】但し、楕円曲線Ｅ上の点Ｐ（≠Ｏ）に対して、$P_x \in Z_q$によりＰのｘ座標を表わす（実施例２参照）。

【０１１２】

【発明の効果】本発明における認証方式によれば、楕円曲線上の離散対数問題に基づいて零知識認証スキームを構築しているので、従来の体上の離散対数問題に基づく零知識認証方式に比べて安全性が向上している。

【０１１３】さらに、証明者と確認者の間の認証処理において、楕円曲線上の点のｘ座標のみの通信で認証プロトコルを構築することができるので、従来の体上の離散対数問題に基づく零知識認証方式と同程度の通信コストで実現できる特徴を持つ。

【０１１４】また、本発明における認証方式では、確認者が証明者を試すために送る乱数の範囲を大きく取れるため、少ない通信回数で不正者の証明者へのなりすまし確率を低く設定することができる。

【０１１５】本発明は、認証処理全般の幅広い範囲に適用できる。特に、本発明は、従来の方式に比べて高い安全性を実現できるため、高度のセキュリティレベルが要求されるシステム、例えば電子投票システムや電子現金システムにおける認証処理に用いて好適である。

【０１１６】また、本発明では、証明者側の秘密情報が少なく、かつ、計算処理負担が小さいため、証明者がＩＣカードを所持し、ＩＣカード内部の秘密情報を利用して認証を行なうシステムにおいても有効である。

【図面の簡単な説明】

【図１】本発明の実施例におけるシステム構成を示す図である。

【図２】本発明のシステム構成内のセンタ側装置の内部構成を示す図である。

【図３】本発明のシステム構成内の証明者側装置の内部構成を示す図である。

【図４】本発明のシステム構成内の確認者側装置を示す図である。

【図５】本発明のシステム構成内のＩＣカードの内部構成を示す図である。

【図６】実施例２の認証方式の概要を示す図である。

【図７】実施例５の認証方式の概要を示す図である。

【符号の説明】

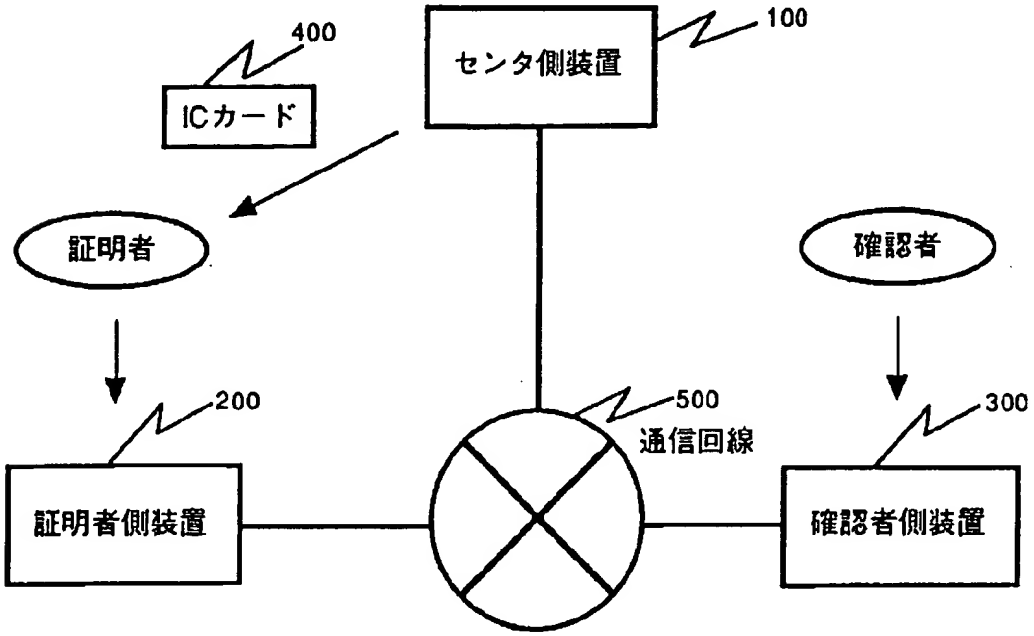
100…センタ側装置、101…センタ側装置100内の入力装置、102…センタ側装置100内の演算装置、103…センタ側装置100内のメモリ、104…センタ側装置100内の乱数生成装置、105…センタ側装置100内の素数生成装置、106…センタ側装置100内の通信装置、107…センタ側装置100内の出力装置、200…証明者側装置、201…証明者側装置200内の入力装置、202…証明者側装置200内のＩＣカード読み書き装置、203…証明者側装置200内の通信装

21

置、204…証明者側装置200内の出力装置、300…確認者側装置、301…確認者側装置300内の入力装置、302…確認者側装置300内の演算装置、303…確認者側装置300内のメモリ、304…確認者側装置300内の乱数生成装置、305…確認者側装置300内の通信装置、306…確認者側装置300内の出力装置、400…ＩＣカード、401…ＩＣカード400内の入力装置、402…ＩＣカード400内の演算装置、403…ＩＣカード400内のメモリ、404…ＩＣカード400内の乱数生成装置、405…ＩＣカード400内の出力装置、500…通信回線。

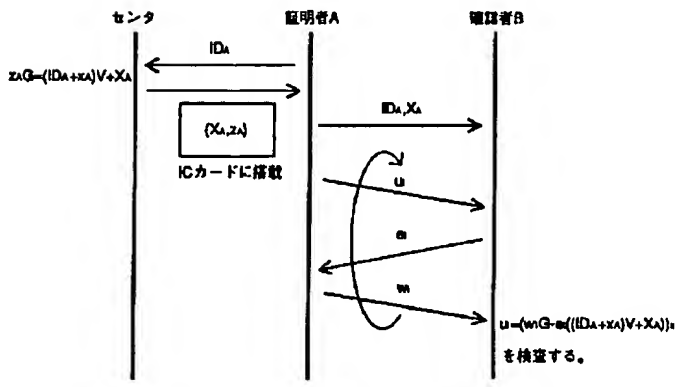
22

【図１】



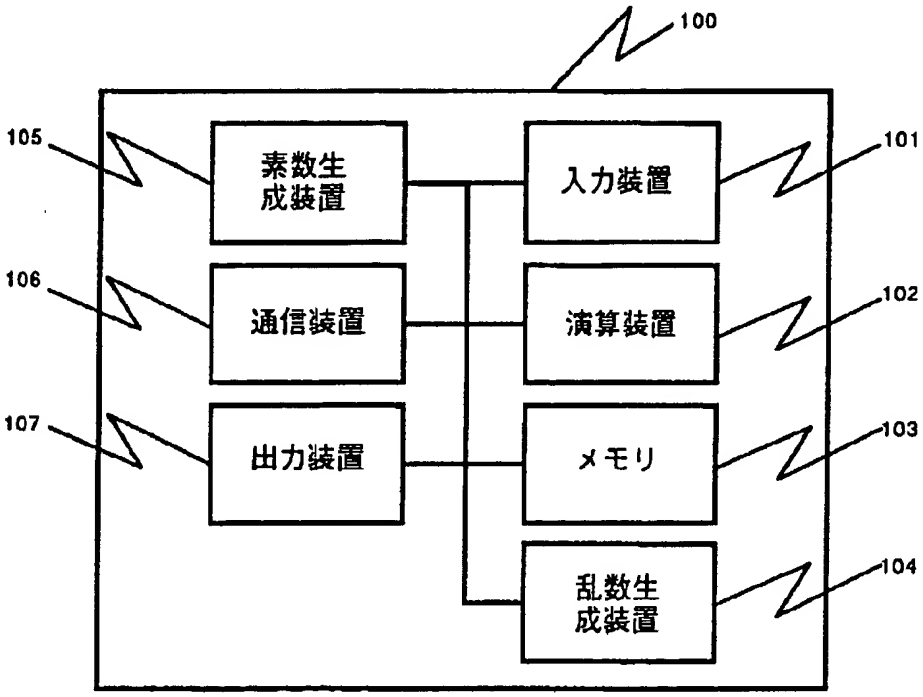
システム構成図

【図６】



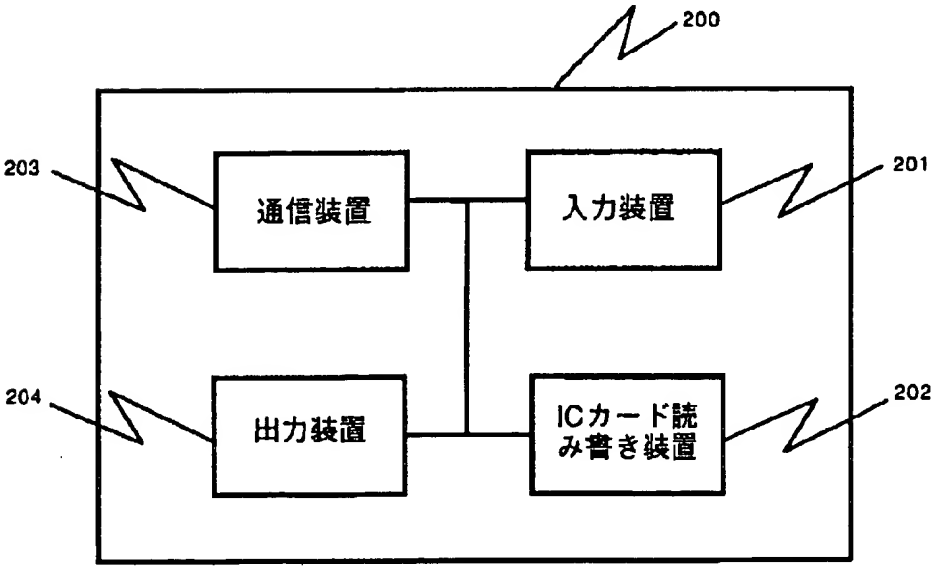
実施例２の処理手順の概要

【図2】



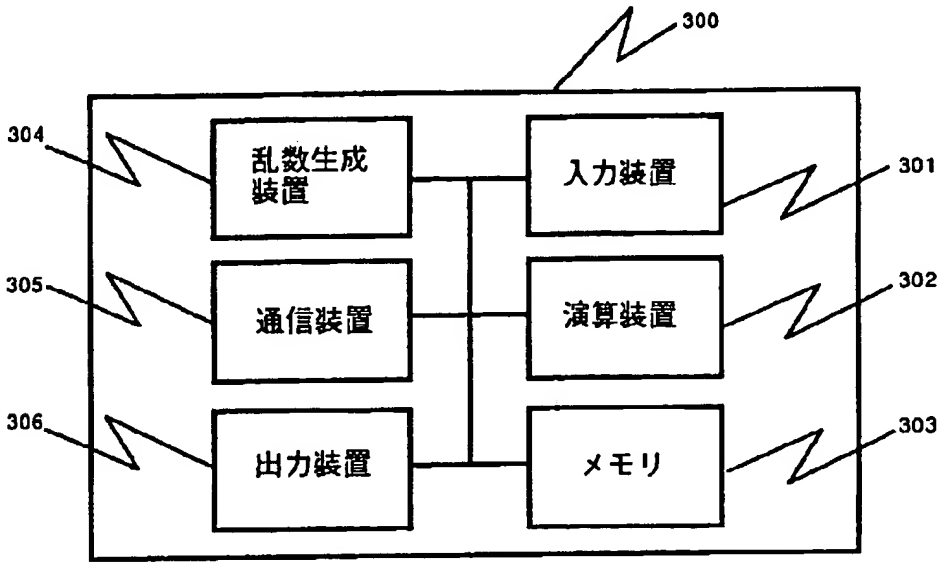
センタ側装置内部構成

【図3】



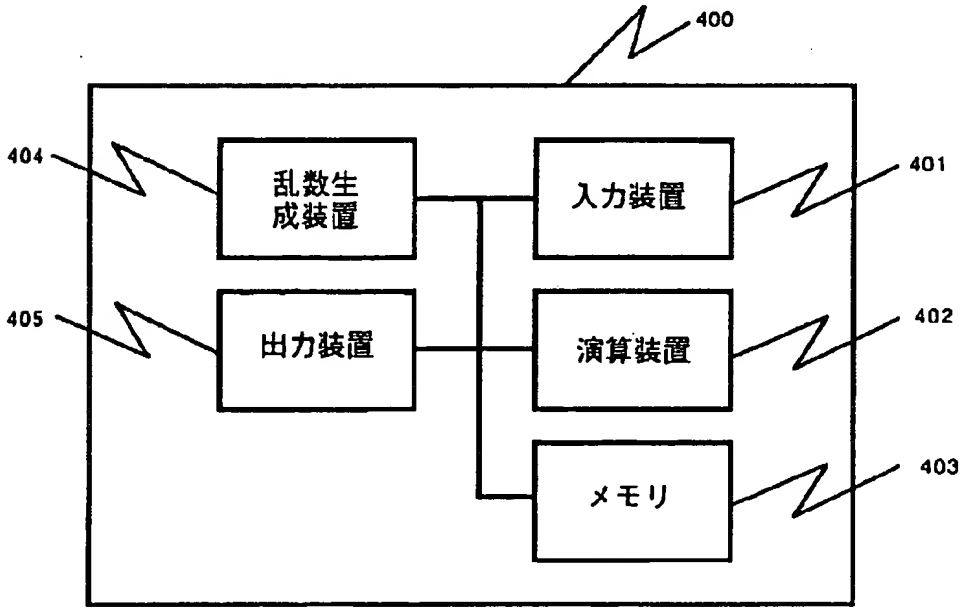
証明者側装置内部構成

【図4】



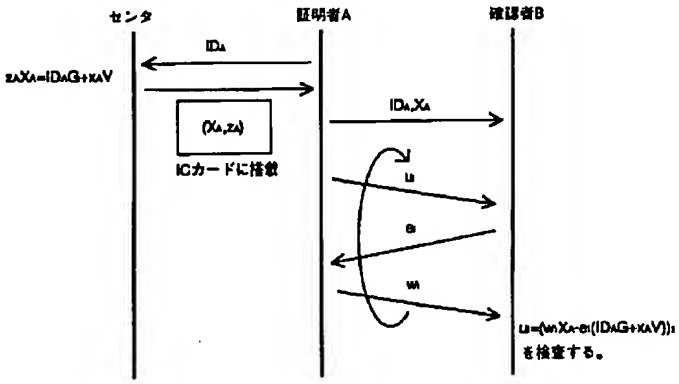
確認者側装置内部構成

【図5】



ICカード内部構成

【図７】



実施例５の処理手順の概要